UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,995	12/01/2003	Nancy Cam Winget	72255/00010	3154

23380 7590 03/18/2008

TUCKER ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
03/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com
mary.erne@tuckerellis.com

Office Action Summary	Application No.	Applicant(s)	
	10/724,995	WINGET ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-21,24,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-21,24,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-12, 14-21, 24, 26, and 27 are pending.

Response to Arguments

1. Applicant's arguments with respect to claims 1-12, 14-21, 24, 26, and 27 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

2. Claims 3, 4, 11, 12, 14, 26, and 27 are objected to because of the following informalities:

- Claim 3 states that “the step of establishing a secure tunnel and receiving a shared secret occurs within a wireless implementation.” There are 3 issues here, first that there are multiple steps, second which "secure tunnel" is being referred to is not clear, and third, since there are multiple steps, they "occur" within a wireless implementation. Therefore, for purposes of prior art rejection, the above has been construed as "the steps of establishing a first secure tunnel and receiving a shared secret occur within a wireless implementation." Claims 4, 11, and 12 have the same issues.
- Claim 14 refers to “the step of establishing a tunnel key”, which is not within claim 1. For purposes of prior art rejection, this has been construed as “the step of deriving a tunnel key”.

- Claim 26 refers to "the wireless device is configured to establish a secure tunnel further comprises", and "employing the secure tunnel". As with claim 3 above, which secure tunnel is being referred to is unclear. For purposes of prior art rejection, this "secure tunnel" has been construed as the “first secure tunnel”.
- Claim 27 refers to the shared secret as being "acquired from the server during provisioning". Since both the server and the provisioning limitation being referred to were removed from claim 1, it is unclear what is meant by this. For purposes of prior art rejection, claim 27 has been construed as ending right after "shared secret".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 9, 10, 12, 14-21, 24, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk (PAUL FUNK, Simon Blake Wilson; “draft-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)”; Internet-Draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40) in view of Kuehr-McLaren (U.S. Patent 6,978,298).

Regarding Claim 1,

Funk discloses a method of authenticating communication between a first and a second party, the method comprising:

Establishing a first secure tunnel between the first party and the second party using asymmetric encryption (Pages 9-10, section 4.3; and Pages 11-13, sections 6-6.2);

Receiving the shared secret via the first secure tunnel between the first party and the second party if a shared secret does not exist (Pages 9-10, section 4.3; and Pages 11-13, sections 6-6.2);

Establishing a subsequent secure tunnel between the first party and the second party using symmetric encryption and the shared secret (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2; and Page 16, section 7);

Mutually deriving a tunnel key for the subsequent secure tunnel using symmetric cryptography based on the shared secret (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2; and Page 16, section 7);

Authenticating a relationship between the first party and the second party within the subsequent secure tunnel (Pages 8-10, sections 4.1-4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10); and

Performing different steps based upon whether the shared secret already exists (Pages 9-15, sections 4.3-6.4);

But does not explicitly disclose a step of determining whether a shared secret exists between a first party and a second party.

Kuehr-McLaren, however, discloses determining whether a shared secret exists between a first party and a second party (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management system of Kuehr-McLaren into the EAP-TTLS system of Funk in order to allow the system to cache session information for a particular amount of time and dynamically modify and/or update the amount of time based upon the needs of the system and its users, thereby allowing for optimized performance while maintaining a high level of security.

Regarding Claim 17,

Claim 17 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user (Pages 9-15, sections 4.3-6.4).

Regarding Claim 3,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that establishing a first secure tunnel and receiving a shared secret occur within a wired implementation (Pages 4-5, section 2).

Regarding Claim 19,

Claim 19 is a system claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 4,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that establishing a first secure tunnel and receiving a shared secret occur within a wireless implementation (Pages 4-5, section 2).

Regarding Claim 18,

Claim 18 is a system claim that corresponds to method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that the shared secret is a protected access credential (PAC) (Pages 9-10, section 4.3; and Pages 11-13, sections 6-6.2).

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Funk as modified by Kuehr-McLaren discloses the method of claim 5, in addition, Funk discloses that the protected access credential includes a protected access credential key (Pages 11-16, sections 6-7).

Regarding Claim 9,

Funk as modified by Kuehr-McLaren discloses the method of claim 6, in addition, Funk discloses that the protected access credential includes a protected access credential opaque element (Pages 3-4, section 1; and Pages 10-13, sections 5-6.2).

Regarding Claim 10,

Funk as modified by Kuehr-McLaren discloses the method of claim 6, in addition, Funk discloses that the protected access credential includes a protected access credential information element (Pages 11-13, sections 6-6.2).

Regarding Claim 12,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that establishing a first secure tunnel and receiving a shared secret occur through in-band mechanisms (Pages 11-13, sections 6-6.2).

Regarding Claim 14,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that deriving a tunnel key further includes establishing a session key seed deriving a master session key used for authenticating the relationship (Pages 11-16, sections 6-7).

Regarding Claim 15,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that the step of authenticating is performed using EAP-GTC (Pages 21-22, section 10.2.1).

Regarding Claim 16,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that the step of authenticating is performed using Microsoft MS-CHAP v2 (Pages 23-24, section 10.2.4).

Regarding Claim 21,

Funk as modified by Kuehr-McLaren discloses the system of claim 18, in addition, Funk discloses that the wireless network is an 802.11 wireless network (Pages 4-5, section 2).

Regarding Claim 24,

Funk discloses a wireless device comprising:

A wireless network adapter for sending and receiving signals with a second wireless device (Pages 4-5, section 2; a wireless network adapter being inherent in wireless communications), wherein the wireless device is configured to:

Receive a shared secret between the wireless device and a second wireless device if a shared secret does not already exist, by establishing a first secure tunnel with a server using asymmetric encryption, wherein the shared secret is received via the first secure tunnel (Pages 9-10, section 4.3; and Pages 11-13, sections 6-6.2);

Establish a subsequent secure tunnel between the wireless device and the second wireless device using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2; and Page 16, section 7);

Mutually authenticate with the second wireless device employing the subsequent secure tunnel (Pages 8-10, sections 4.1-4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10); and

Performing different steps based upon whether the shared secret already exists (Pages 9-15, sections 4.3-6.4);

But does not explicitly disclose a step of determining whether a shared secret exists between a first party and a second party.

Kuehr-McLaren, however, discloses a wireless network adapter (Column 4, lines 37-52; and Column 10, line 62 to Column 11, line 11); and determining whether a shared secret exists between a first party and a second party (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32). It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to incorporate the session management system of Kuehr-McLaren into the EAP-TTLS system of Funk in order to allow the system to cache session information for a particular amount of time and dynamically modify and/or update the amount of time based upon the needs of the system and its users, thereby allowing for optimized performance while maintaining a high level of security.

Regarding Claim 26,

Funk as modified by Kuehr-McLaren discloses the device of claim 24, in addition, Funk discloses that establishing a first secure tunnel further comprises establishing a session key seed for deriving a master session key used for mutually authenticating the second wireless device employing the first secure tunnel (Pages 11-16, sections 6-7).

Regarding Claim 27,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses establishing a plurality of subsequent secure tunnels between the first party and second party using the shared secret (Pages 11-15, sections 6-6.4); and Kuehr-McLaren discloses establishing a plurality of subsequent secure tunnels between the first party and second party using the shared secret (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32).

4. Claims 5-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk in view of Kuehr-McLaren, further in view of Downnard (Downnard, Ian, "Public-key cryptography extensions into Kerberos", IEEE, December 2002/January 2003, pp. 30-34).

Regarding Claim 5,

Funk as modified by Kuehr-McLaren discloses the method of claim 1, in addition, Funk discloses that the shared secret is a protected access credential (PAC) (Pages 9-10, section 4.3; and Pages 11-13, sections 6-6.2); but does not explicitly disclose certain specifics of such a PAC.

Downnard, however, discloses that the shared secret is a protected access credential (PAC) (Pages 30 and 32, Kerberos and PKINIT sections). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the public-key-extended Kerberos system of Downnard into the EAP-TTLS system of Funk as modified by Kuehr-McLaren in order to ensure authentication of the entities wishing to communicate as well as a trusted party that distributes shared secret information, while improving security and scalability through use of public keys for initial authentication.

Regarding Claim 6,

Funk as modified by Kuehr-McLaren and Downnard discloses the method of claim 5, in addition, Downnard discloses that the protected

access credential includes a protected access credential key (Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 7,

Funk as modified by Kuehr-McLaren and Downnard discloses the method of claim 6, in addition, Funk discloses that the protected access credential key is a strong entropy key (Page 16, section 7); and Downnard discloses that the protected access credential key is a strong entropy key (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 8,

Funk as modified by Kuehr-McLaren and Downnard discloses the method of claim 7, in addition, Downnard discloses that the entropy key is a 32 octet key (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 9,

Funk as modified by Kuehr-McLaren and Downnard discloses the method of claim 6, in addition, Downnard discloses that the protected access credential includes a protected access credential opaque element (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 10,

Funk as modified by Kuehr-McLaren and Downnard discloses the method of claim 6, in addition, Downnard discloses that the protected

access credential includes a protected access credential information element (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 11,

Funk as modified by Kuehr-McLaren does not explicitly disclose that establishing a first secure tunnel and receiving a shared secret occur through out-of-band mechanisms.

Downnard, however, discloses that establishing a first secure tunnel and receiving a shared secret occur through out-of-band mechanisms (Pages 30 and 32, Kerberos and PKINIT sections). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the public-key-extended Kerberos system of Downnard into the EAP-TTLS system of Funk as modified by Kuehr-McLaren in order to ensure authentication of the entities wishing to communicate as well as a trusted party that distributes shared secret information, while improving security and scalability through use of public keys for initial authentication.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

/Jeffrey D Popham/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137